

CODES ON VARIETIES AS CODES ON CURVES

SRIMATHY SRINIVASAN

ABSTRACT. The discovery of algebraic geometric codes constructed on curves led to generalising this construction on higher dimensional varieties. In this paper, we use a theorem of B. Poonen to show that the codes obtained from higher dimensional varieties can be realised as codes on curves. One of the important consequences of this result is that the search for good codes on varieties that beat the existing bounds can be restricted to the case of curves.

1. INTRODUCTION

Coding theory, the study of designing efficient codes that help in reliable data transmission, is an integral component of any communication system. The basic idea is to “encode” the q -ary message to be transmitted by adding redundant information to immunize against errors and “decode” at the receiver thereby achieving reliability.

One way to encode is by linearly embedding the k bit message space \mathbb{F}_q^k into \mathbb{F}_q^n and transmit the vectors in the image of the embedding. We call the image a *code* and the vectors in it *codewords*. *Minimum distance* d , the minimum number of positions in which any two distinct codes differ, is an important parameter of a code that measures its error correcting capability. Typically, we need codes with relative parameters $\delta = \frac{d}{n}$ and $R = \frac{k}{n}$ to be as large as possible. In fact, one of the important problems in coding theory is to construct a sequence of codes with $n \rightarrow \infty$ such that the limit (δ, R) of relative parameters is non-zero. Such a sequence of codes is called a sequence of *good codes*.

It is well known that the maximal achievable R for a given δ , denoted as $\alpha_q(\delta)$, is a continuous decreasing function of δ . Although the exact function $\alpha_q(\delta)$ is not known, there are many lower bounds for it. One significant bound is the *Gilbert-Varshamov* bound which was known to be the best until *Algebraic Geometric Codes* were discovered. These codes are constructed by picking rational points on smooth projective curves and evaluating global sections of a line bundle at these points. The parameters of these codes are easily estimated using the Riemann-Roch theorem and good parameters can be obtained by choosing good curves with many rational points. One such example of a family of good curves is the family of *modular curves*. These curves have a lot of rational points thereby yielding a good family of codes that beat the Gilbert-Varshamov bound.

One can generalize the construction of codes on curves to codes on surfaces or any other higher dimensional variety in an analogous manner: Pick a set of \mathbb{F}_q rational points on the variety and evaluate the global sections of a line bundle at these points to get a linear code. In this case, estimating the parameters of the code is harder than in the case of curves as we need Riemann-Roch in higher dimensions. However, one possible direction to tackle the problem is to realise the codes on the varieties as codes on curves whose parameters can be estimated easily. We show that codes on higher dimensional varieties can be realised as codes on curves. This can be done using a theorem of Poonen’s [2]. Although there are papers [4] that use Poonen’s theorem to obtain results on algebraic geometric codes, there does not seem to be any literature that states this result. An interesting corollary of this method is that, since every algebraic geometric code on a higher dimensional variety can be realised as a code on some curve, good codes that are achievable through higher dimensional varieties are achievable through curves and hence we can restrict our focus on curves in our search for good codes and the codes that beat existing bounds.

2. CODING THEORY BACKGROUND

An $(n, k, d)_q$ -code is a k -dimensional subspace of an n -dimensional vector space over \mathbb{F}_q . The vectors in a code are called *codewords*. The parameter d is called the *minium distance*. It is the minimum of Hamming distances between any two distinct codewords. Since a code is a linear subspace, it is also equal to the minimum of Hamming weights of all the non-zero codewords. Finding minimum distance given a basis for the code is NP - hard. For practical purposes we need the dimension k and the minimum distance d of a code to be large as possible for a given length. So for an $(n, k, d)_q$ - code C , we define the *relative dimension* or *code rate*, $R(C) = \frac{k}{n}$ and *relative minimum distance*, $\delta(C) = \frac{d}{n}$. The pair $(\delta(C), R(C))$ denotes a point in $[0, 1] \times [0, 1]$. A sequence of codes $\{C_i\}$ is said to be *asymptotically good* if $\lim_{i \rightarrow \infty} \delta(C_i) > 0$ and $\lim_{i \rightarrow \infty} R(C_i) > 0$.

Define,

$$U_q = \{(\delta, R) \mid \text{there exists a sequence of codes } \{C_i\} \text{ with } \lim_{i \rightarrow \infty} (\delta(C_i), R(C_i)) = (\delta, R)\}$$

Then, it is know that there is a *continuous decreasing* function $\alpha_q(\delta)$ such that $U_q = \{(\delta, R) \mid 0 \leq R \leq \alpha_q(\delta)\}$. The exact function $\alpha_q(\delta)$ is unknown although few upper and lower bounds for the function is known. One lower bound is given by the Gilbert-Varshamov(GV) bound, $R_{GV}(\delta) \leq \alpha_q(\delta)$, where

$$R_{GV}(\delta) = 1 - (\delta \cdot \log_q(q-1) - \delta \cdot \log_q(\delta) - (1-\delta) \cdot \log_q(1-\delta))$$

It was the best known bound for many years until the invention of *Algebraic Geometric (AG) Codes* which beat the GV bound.

3. ALGEBRAIC GEOMETRIC CODES ON CURVES

Algebraic Geometric codes were first dicovered by Goppa [3] and was further developed by many coding theorists and mathematicians along the way. In this section, we follow the notations from [1].

Let X be a smooth projective curve of genus g over \mathbb{F}_q and let $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ be a subset of \mathbb{F}_q points on X . Suppose D is a divisor on X such that $0 \leq \deg D = a < n = |\mathcal{P}|$ and $\text{supp } D \cap \mathcal{P} = \emptyset$. We have the space of global sections given by

$$H^0(\mathcal{L}(D)) = \{f \in \mathbb{F}_q(X)^* \mid (f) + D \geq 0\} \cup \{0\}.$$

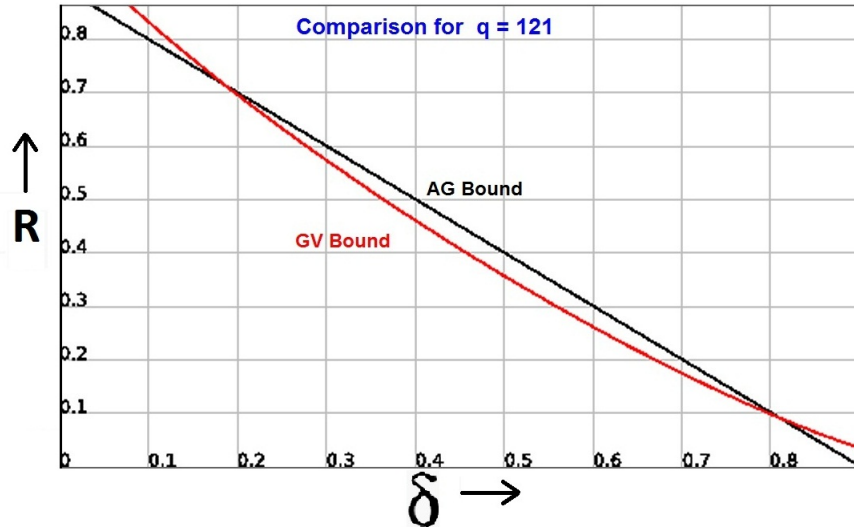
Consider the *evaluation map*:

$$\begin{aligned} \text{Ev}_{\mathcal{P}} : \mathcal{L}(D) &\longrightarrow \mathbb{F}_q^n \\ \text{Ev}_{\mathcal{P}} : f &\longmapsto [f(P_1), f(P_2), \dots, f(P_n)] \end{aligned}$$

The image of the map gives a linear code $C(X, \mathcal{P}, \mathcal{L}(D)) = \text{Ev}_{\mathcal{P}}(\mathcal{L}(D))$. (Note: One can also get an "equivalent code" by choosing a trivialization and evaluating the global sections at the stalks). The parameters of this code satisfy $k + d \geq n - g + 1$ where n is the length of the code, k its dimension and d the minimum distance.

When $q = p^{2m}$, one can construct these codes on Modular and Drinfeld curves with good asymptotic behavior. In particular, we get the *Algebraic Geometry (AG) Bound*, $\alpha_q(\delta) \geq 1 - \frac{1}{\sqrt{q}-1} - \delta$ which beats the Gilbert-Varshamov Bound.

The AG-bound beats the GV-bound in a region along δ for $q \geq 49$.



4. CODES ON HIGHER DIMENSIONAL VARIETIES AS CODES ON CURVES

We can imitate construction of codes on curves to get codes on higher dimensional smooth varieties by choosing a set of rational points and a line bundle together with a trivialization. In this case, estimating the parameters of the code is not so easy as we have to invoke Riemann-Roch in higher dimensions where the higher cohomology groups come into picture. However, we will show that the codes thus obtained can also be realised as codes on some curve of high enough degree. This curve comes from a result in Poonen's paper [2], which we recall for the convenience of the reader.

Theorem (Poonen). *Let X be a smooth projective geometrically integral variety of \mathbb{P}^n of dimension $m \geq 1$ over \mathbb{F}_q , and let $\mathcal{P} \subset X$ be a finite set of closed points. Then, given any integer d_0 , there exists a smooth projective geometrically integral hypersurface $H \subset \mathbb{P}^n$ of degree $d \geq d_0$ such that $Y = H \cap X$ is smooth projective and geometrically integral of dimension $m - 1$ and contains \mathcal{P} .*

Example. Consider $X = \mathbb{P}^2$ over \mathbb{F}_2 . Let \mathcal{P} be the set of all 7 \mathbb{F}_2 points. Then, the curve $Y = yz^3 + y^3z + xy^3 + x^2z^2 + x^2y^2 + x^3z$ is a smooth curve passing through \mathcal{P} . In fact, one can show that there are 24 smooth curves of degree 4 passing through \mathcal{P} .

Suppose $C(X, \mathcal{P}, \mathcal{L})$ is a code on a geometrically integral smooth projective variety $X \subseteq \mathbb{P}^n$ of dimension $m \geq 2$ over \mathbb{F}_q . Here \mathcal{L} is the corresponding line bundle and \mathcal{P} the corresponding subset of \mathbb{F}_q -points. Let $Y = H \cap X$ be as above with degree d of H large enough. Then, we have an exact sequence

$$0 \longrightarrow \mathcal{I}_Y \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_Y \longrightarrow 0$$

where $\mathcal{I}_Y = \mathcal{O}_X(-d)$. Tensoring with \mathcal{L} we get

$$0 \longrightarrow \mathcal{L} \otimes \mathcal{I}_Y \longrightarrow \mathcal{L} \longrightarrow \mathcal{L} \otimes \mathcal{O}_Y \longrightarrow 0.$$

This gives rise to a long exact sequence in cohomology on X ,

$$0 \longrightarrow H^0(\mathcal{L} \otimes \mathcal{I}_Y) \longrightarrow H^0(\mathcal{L}) \longrightarrow H^0(\mathcal{L} \otimes \mathcal{O}_Y) \longrightarrow H^1(\mathcal{L} \otimes \mathcal{I}_Y) \longrightarrow \dots$$

By duality, we have

$$H^i(\mathcal{L} \otimes \mathcal{I}_Y) = H^{m-i}(\omega_X \otimes \mathcal{I}_Y^\vee \otimes \mathcal{L}^\vee) = H^{m-i}(\omega_X \otimes \mathcal{L}^\vee \otimes \mathcal{O}_X(d))$$

where ω_X is the canonical sheaf on X . Since $\mathcal{O}_X(1)$ is ample, for large enough d , $H^0(\mathcal{L} \otimes \mathcal{I}_Y)$ and $H^1(\mathcal{L} \otimes \mathcal{I}_Y)$ vanishes and we get a canonical isomorphism obtained via restriction

$$\begin{aligned} H^0(\mathcal{L}) &\xrightarrow{\sim} H^0(\mathcal{L} \otimes \mathcal{O}_Y) \\ f &\longmapsto f|_Y. \end{aligned}$$

Inducting the above argument by replacing the m -dimensional variety X with $(m - 1)$ -dimensional variety Y and \mathcal{L} with $\mathcal{L} \otimes \mathcal{O}_Y$ we obtain the following:

Theorem. *Let X be a smooth projective geometrically integral variety over the finite field \mathbb{F}_q and let \mathcal{L} be a line bundle on X . Then there exists a smooth projective curve Y passing through a given set \mathcal{P} of \mathbb{F}_q points of X and such that the restriction map $H^0(X, \mathcal{L}) \rightarrow H^0(Y, \mathcal{L} \otimes \mathcal{O}_Y)$ is an isomorphism. This yields a code $C(Y, \mathcal{P}, \mathcal{L} \otimes \mathcal{O}_Y)$ on Y which is the same as the code $C(X, \mathcal{P}, \mathcal{L})$ on X .*

Hence, given a code on a geometrically integral smooth projective variety, we have realised it over a smooth projective curve. We can therefore restrict our attention to curves in our search for good codes and codes meant to beat the existing bounds on $\alpha_q(\delta)$.

ACKNOWLEDGEMENTS. I would like to thank Prof. Patrick Brosnan and Prof. Lawrence Washington for their valuable comments and discussions. I would also like to thank Richard Rast for writing a computer program to verify some results.

REFERENCES

- [1] M.A Tsfasman, S.G Vladut *Algebraic - Geometric Codes*, Springer, 1991.
- [2] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) 160 (2004), no. 3, 1099-1127
- [3] V.G. Goppa, *Codes on algebraic curves* Soviet Math. Dokl, 24 (1981), 170-172
- [4] Couvreur, Alain *Differential approach for the study of duals of algebraic-geometric codes on surfaces*, J. Thor. Nombres Bordeaux 23 (2011), no. 1, 95-120.

DEPARTMENT OF MATHEMATICS, 1301 MATHEMATICS BUILDING, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742-4015, USA